Chapter 2
Efficient Anonymous and Non-Repudiation E-Payment Protocol

Sattar J. Aboud
Iraqi Council of Representatives, Iraq

ABSTRACT

There are many proposals which offer anonymous and non-repudiation e-payment protocols. But they have the drawbacks that the anonymity can be misused fraudulently to perform a perfect crime. Currently, the hot research concentrates on the accepting of e-payment protocols where the anonymity of the coins is cancelable via a trusted authority in the case of criminal entities. In the chapter the author suggests an efficient protocol for e-payment schemes that offers a good level of security with appreciate to its efficiency. The proposed protocol prevents the blind office and the bank from impersonating an entity, so that the entity could not repudiate it when the entity misused a coin. Another benefit is that it is constructed from efficient cryptography schemes so that its security can simply be analyzed. The strength of this scheme is in its easiness. So, the author claims that the suggested protocol is more efficient than the existing schemes, since it allows to both a blind office and a bank to impersonate an entity to find and to spend a coin without to be noticed. It might cause a repudiation difficulty where the entity can repudiate his bad activities by proposing that both the bank and the blind office acted inaccurately. Other relevant issues related to the new protocol will be discussed in the section of the security of the scheme.

INTRODUCTION

Internet is designed to allow computers to easily interconnect and to assure that network connections will be maintained even when various links may be damaged, but this versatility also makes it easy to compromise data security and privacy protection for e-commerce application. E-payment systems allow people to carry out commercial activities in an electronic domain. There are many electronic payment systems that have been proposed in recent years (Liu et al., 2001). A secure e-payment systems protecting privacy can be seen as a protocol involving a
Efficient Anonymous and Non-Repudiation E-Payment Protocol

customer, a shop and a bank. It is goal to transfer money in a secure way from the customer’s account to the shop’s account. E-payment systems are conventionally divided into those that are on-line and those that are off-line, one can distinguish between on-line payments systems where all parties, the customer, the shop and bank need to be connected on-line, and off-line payments system, where each interaction during the protocol requires two communicating parties only (Camenisch, & Stadler, 1996).

E-payment is a subject of great economic, political and research and Security is an important factor for the wide acceptance of the electronic commerce services. There are many proposals discussed the e-payment protocols which enable anonymity services to protect user’s privacy. Protocols relying on traditional trusted parties easily guarantee exchanges, but are inefficient -because a trusted party must be part of every transaction and expensive because a trusted party wants to be paid for each transaction.

Anonymity of the participant’s is an important requirement for electronic commerce, in particular for payment systems, because anonymity could be in conflict with law enforcement, currently the researches concentrate on accepting of e-payment protocols where the anonymity of the coins is cancellable via a trustee in case of criminal entities. Most of current systems have drawbacks that the anonymity can be misused by fraudulent to perform a perfect crimes like blackmailing or money laundering and do not provide the non-repudiation service which prevent users from repudiate the misusing of the coins like denying, double-spending.

The idea of anonymous payment scheme was introduced in 1982 (Chaum, 1983). In fact this anonymity might be misused by fraudulent to perform a perfect crime (Solms & Naccache, 1992). For instance stealing of the private keys, money laundry, and blackmailing of coins. The uses of blindfolded protocols in the banks are considered as a modern threat (Liu et al., 2001). To avoid these threats the payment schemes must offer anonymity method which accepts the tracing of coins in any of the states mentioned above by an authorized trusted authority. The first scheme that is stopping blackmailing and money laundry was suggested in (Brickell et al., 1995). However, there are some proposals (Camenisch, 1996; M’Raihi, 1996; Jacobson & Youg, 1997) to prevent these threats. Every scheme needs the participation of the trusted authority in the opening of the bank account, and also in the withdrawal of coins. The only scheme that does not need trusted authority participation excepting the anonymity has just suggested in (Binh, 2007). But, it is unable to stop extortion threats and the employ of blindfolding schemes. These threats are just prevented in the scheme of (Hohenberger, 2006), which is also not efficient as it needs the trusted authority interaction in e-payment schemes. In case that one of these threats is needed, they require an on-line e-payment scheme among user, shop, and trusted authority to stop the spending of illegitimate coins.

Chaum, Fiat and Naor proposed a practical electronic cash system, using the blind signature paradigm to provide privacy and security for all involved parties (Chaum et al., 1988). However, while protecting the honest customer’s privacy in fact the perfect anonymity obtained through the usage of blind signature also open doors for misuse by fraudulent to perform a perfect crime as mentioned in (Solms, & Naccache, 1992). Brickell, Gemmell and Kravitz proposed a new scheme to avoid threats obtained from using a perfect anonymity like blackmailing and money laundry by involving an authorized trustee during withdrawal that can revoke anonymity of certain transaction as needed (Brickell et al., 1995).

The concept of anonymity-revocable payment systems, sometimes called fair payment system, that enables the trustee to revoke customer’s anonymity in cooperation with the bank, but the customer’s privacy cannot be compromised by the
Related Content

Supporting Entrepreneurship in High Cost Economies: What Can Governments Do?
Allan O'Connor, Graciela Corral de Zubielqui, Mushui Huanmei Li and Manjula Dissanayake (2014). Global Perspectives on Achieving Success in High and Low Cost Operating Environments (pp. 290-392).
www.igi-global.com/chapter/supporting-entrepreneurship-in-high-cost-economies/106802?camid=4v1a

Carbon-Efficient Supply Chains
www.igi-global.com/article/carbon-efficient-supply-chains/134861?camid=4v1a

How Firm and Market Characteristics Affect Profitability: An Empirical Study
www.igi-global.com/article/how-firm-and-market-characteristics-affect-profitability/134864?camid=4v1a

The Determinants of Stock Market Development in Emerging Economies: Examining the Impact of Corporate Governance and Regulatory Reforms (II)
www.igi-global.com/chapter/the-determinants-of-stock-market-development-in-emerging-economies/173102?camid=4v1a